

PATENT COOPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:

LAZAR, D.S.
CUSHMAN DARBY & CUSHMAN
1100 NEW YORK AVENUE, N.W.
WASHINGTON, D.C. 20005
ETATS-UNIS D'AMERIQUE

PCT

NOTIFICATION OF TRANSMITTAL OF
THE INTERNATIONAL PRELIMINARY
EXAMINATION REPORT
(PCT Rule 71.1)

Date of mailing
(day/month/year)

23. 02. 99

Applicant's or agent's file reference
Certco214606

IMPORTANT NOTIFICATION

International application No.
PCT/US97/22136

International filing date (day/month/year)
11/12/1997

Priority date (day/month/year)
13/12/1996

Applicant
CERTCO, LLC et al.

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.
2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.
3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.
4. **REMINDER**

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/



European Patent Office
D-80298 Munich
Tel. (+49-89) 2399-0 Tx: 523656 epmu d
Fax: (+49-89) 2399-4465

Authorized officer

Condron, M

Tel. (+49-89) 2399-2296



PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference Certco214606	FOR FURTHER ACTION		See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/US97/22136	International filing date (day/month/year) 11/12/1997	Priority date (day/month/year) 13/12/1996	
International Patent Classification (IPC) or national classification and IPC G07F19/00			
Applicant CERTCO, LLC et al.			

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.


2. This REPORT consists of a total of 6 sheets, including this cover sheet.

- ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 10 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 08/07/1998	Date of completion of this report 23. 02. 99
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. (+49-89) 2399-0 Tx: 523656 epmu d Fax: (+49-89) 2399-4465	Authorized officer Rahner, H-G Telephone No. (+49-89) 2399 2773



**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/US97/2213r

I. Basis of the report

1. This report has been drawn on the basis of *(substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.)*:

Description, pages:

1-103	as originally filed		
16a-16c	as received on	23/11/1998 with letter of	18/11/1998

Claims, No.:

1-30	as received on	23/11/1998 with letter of	18/11/1998
------	----------------	---------------------------	------------

Drawings, sheets:

1/12-12/12	as originally filed
------------	---------------------

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/US97/22137

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-30
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-30
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-30
	No:	Claims	

2. Citations and explanations

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/US97/22136

Re Item V

Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

- 1). Reference is made to the following documents:

D1: M. Bellare et al.: "iKP- A Family of Secure Electronic Payment Protocols";
Proceedings of the USENIX Workshop on Electronic Commerce; 11 July
1995; pages 89-106; XP000579445.

D2: WO-A-96/21192

- 2). In a conventional approach to digital signature certification the problem exists that the certification authority's service contract is entirely with the subscriber, although the relying party, who bears the greatest risk of fraud or forgery in the transaction, has the highest interest in the information security of the transaction.

The present invention as defined in the independent claims 1, 8, 14 and 21, relating to electronic transactions supporting reliance on digital signature certificates and managing the risk of such certificates, aims at a solution to this problem.

In particular, it is suggested that

- a certification authority generates electronic signals representing subscriber assurance of an attribute of a subscriber to the system, that
- a reliance server obtains information regarding said subscriber assurance, and that
- the reliance server issues electronic signals representing transactional assurance to a relying party.

The key function of the reliance server is therefore to assure that the relying party has properly enrolled into the system and that transactional assurance is based on the subscriber attribute assurance.

- 3). The available relevant prior art is disclosed in documents D1 and D2.

D1, in particular the paragraph bridging pages 89 and 90, contains a general discussion on secure electronic payment protocols, between relying parties (customer - merchant - acquirer [= gateway to existing clearing/authorization network]). All parties are previously provided (probably from a certification authority) with certificates, including Ks/Kp.

D2 (e.g. the abstract) concerns the electronic sale of goods. On receiving a request from a buyer, the clearinghouse makes a determination of the risk classification and transfers the payment amount (minus discount fee, depending on that classification) to the seller's account, and an invoice, for the purchase price, to the buyer.

- 4). The specific combination of the features as suggested in the independent claims 1, 8, 14 and 21 does not follow in an obvious manner from the available state of the art.

The requirements of Article 33(2) and (3) PCT regarding novelty and inventive step are therefore met.

Dependent claims 2-7, 9-13, 15-20 and 22-30 relate to embodiments of the invention defined in the independent claims and likewise meet the requirements of Article 33(2) and (3) PCT.

Industrial applicability of the claimed subject-matter appears obvious (Article 33(4) PCT).

Re Item VII

Certain defects in the international application

- 5). The description is not in conformity with the current claims as required by Rule 5.1(a)(iii) PCT.
For example, the description on page 8, line 21 to page 16, line 29 and page 17, line 1-25 still recites the wording of previous claims leading to an inconsistency between claims and description.

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/US97/22136

Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the documents D1 and D2 is not mentioned in the description, nor are these documents identified therein.

In another aspect, this invention is an electronic transaction system. The system comprises an authority and a reliance server. The authority generates electronic signals representing subscriber assurance of an attribute of a subscriber to the system; and the reliance server obtains electronic signals representing information regarding the subscriber assurance issued by the authority. The reliance server issues electronic signals representing transactional assurance to a relying party, the transactional assurance being based at least on the subscriber attribute assurance. In another aspect, this invention is a method of managing reliance in an electronic transaction system. In some embodiments, the method comprises, by an authority, generating electronic signals representing subscriber assurance of an attribute of a subscriber to the system; and, by a reliance server, obtaining electronic signals representing information regarding the subscriber assurance issued by the authority, and issuing electronic signals representing transactional assurance to a relying party, the transactional assurance being based at least on the subscriber attribute assurance.

In some embodiments the subscriber assurance comprises at least one of (a) an identification assurance of the identity of the subscriber and (b) an authorization assurance of authorization of the subscriber. In some embodiments, the subscriber assurance comprises electronic signals representing a certificate. In some other embodiments, the reliance server issues electronic signals representing assurance to the relying party based also on information provided by the relying party. In some other embodiments, the request for transactional assurance comes from the relying party, sometimes directly. In some embodiments, the reliance server issues the electronic signals representing the transactional assurance directly to the relying party.

GEÄNDERTES BLATT

In another aspect, this invention is a method of managing reliance in an electronic transaction system in which an authority issues subscriber assurance of an attribute of a subscriber to the subscriber. The method comprises receiving electronic signals representing a transaction associated with a subscriber, the transaction including information regarding at least one attribute of that subscriber; creating a reliance request message specifying at least one aspect of the transaction upon which a relying party intends to rely; and causing electronic signals representing the reliance request message to be sent to a reliance server requesting a transactional assurance for the aspect of the transaction upon which the relying party intends to rely. In some embodiments, the method further includes receiving electronic signals representing a transactional assurance from the reliance server; and continuing the transaction with the subscriber based on information in the transactional assurance. Sometimes the electronic signals representing the transactional assurance are received in response to the sending of the reliance request message.

In some cases the subscriber assurance comprises at least one of (a) an identification assurance of the identity of the subscriber and (b) an authorization assurance of authorization of the subscriber.

The reliance request message can come from the relying party, directly or indirectly.

The reliance server can issue the electronic signals representing the transactional assurance directly to the relying party.

In yet another aspect, this invention is a method of managing reliance in an electronic transaction system in which an authority issues subscriber assurance of an attribute of a subscriber to the subscriber. The method includes receiving

electronic signals representing a reliance request message, the message specifying an aspect of a transaction with a subscriber upon which a relying party intends to rely and requesting assurance for the aspect of the transaction; determining whether to provide transactional assurance based on the reliance request message;
5 and generating electronic signals representing an indication of whether transactional assurance is available.

In some embodiments, the method further includes receiving electronic signals representing the transactional assurance; and continuing the transaction based on information in the transactional assurance.

10 The electronic signals representing the transactional assurance may be received in response to the sending of the request message.

The subscriber assurance may comprise at least one of (a) an identification assurance of the identity of the subscriber and (b) an authorization assurance of authorization of the subscriber. The reliance request message comes from the
15 relying party, directly or indirectly. The electronic signals representing the transactional assurance may be issued directly to the relying party. The reliance request message may include certificate information derived from the transaction and the determining whether to provide the transactional assurance may further comprise determining the status of certificates associated with the transaction.
20 This may include determining whether certificates associated with the transaction have been revoked or suspended.

What is claimed:

1. An electronic transaction system comprising:
an authority generating electronic signals representing
5 subscriber assurance of an attribute of a subscriber to the system; and
a reliance server obtaining electronic signals representing
information regarding the subscriber assurance issued by the
authority, the reliance server issuing electronic signals representing
transactional assurance to a relying party, the transactional assurance
10 being based at least on the subscriber attribute assurance.
2. A system as in claim 1 wherein the subscriber assurance
comprises at least one of (a) an identification assurance of the
identity of the subscriber and (b) an authorization assurance of
15 authorization of the subscriber.
3. A system as in claim 1 wherein the subscriber assurance
comprises electronic signals representing a certificate.
- 20 4. A system as in claim 1 wherein the reliance server issues
electronic signals representing assurance to the relying party based
also on information provided by the relying party.
5. A system as in claim 1 wherein the request for
25 transactional assurance comes from the relying party.

6. A system as in claim 4 wherein the request for transactional assurance comes directly from the relying party.

7. A system as in claim 1 wherein the reliance server issues the electronic signals representing the transactional assurance directly to the relying party.

8. A method of managing reliance in an electronic transaction system, the method comprising:

by an authority, generating electronic signals representing subscriber assurance of an attribute of a subscriber to the system; and by a reliance server,

obtaining electronic signals representing information regarding the subscriber assurance issued by the authority, and issuing electronic signals representing transactional assurance to a relying party, the transactional assurance being based at least on the subscriber attribute assurance.

9. A method as in claim 8 wherein the subscriber assurance comprises at least one of (a) an identification assurance of the identity of the subscriber and (b) an authorization assurance of authorization of the subscriber.

10. A method as in claim 8 wherein the subscriber assurance comprises electronic signals representing a certificate.

11. A method as in claim 8 wherein the reliance server issues electronic signals representing assurance to the relying party based also on information provided by the relying party.

12. A method as in claim 8 wherein the request for transactional assurance comes from the relying party.

13. A method as in claim 12 wherein the request for transactional assurance comes directly from the relying party.

14. A method of managing reliance in an electronic transaction system in which an authority issues subscriber assurance of an attribute of a subscriber to the subscriber, the method comprising:

receiving electronic signals representing a transaction associated with a subscriber, the transaction including information regarding at least one attribute of that subscriber;

creating a reliance request message specifying at least one aspect of the transaction upon which a relying party intends to rely; and

causing electronic signals representing the reliance request message to be sent to a reliance server requesting a transactional assurance for the aspect of the transaction upon which the relying party intends to rely.

15. A method as in claim 14 further comprising:

receiving electronic signals representing a transactional
assurance from the reliance server; and

5 continuing the transaction with the subscriber based on
information in the transactional assurance.

16. A method as in claim 15 wherein the electronic signals
representing the transactional assurance are received in response to
10 the sending of the reliance request message.

17. A method as in claim 14 wherein the subscriber
assurance comprises at least one of (a) an identification assurance of
the identity of the subscriber and (b) an authorization assurance of
15 authorization of the subscriber.

18. A method as in claim 14 wherein the reliance request
message comes from the relying party.

20 19. A method as in claim 14 wherein the request message
comes directly from the relying party.

20. A method as in claim 14 wherein the reliance server
issues the electronic signals representing the transactional assurance
25 directly to the relying party.

21. A method of managing reliance in an electronic transaction system in which an authority issues subscriber assurance of an attribute of a subscriber to the subscriber, the method comprising:

receiving electronic signals representing a reliance request message, the message specifying an aspect of a transaction with a subscriber upon which a relying party intends to rely and requesting assurance for the aspect of the transaction;

determining whether to provide transactional assurance based on the reliance request message; and

generating electronic signals representing an indication of whether transactional assurance is available.

22. A method as in claim 21 further comprising:

receiving electronic signals representing the transactional assurance; and

continuing the transaction based on information in the transactional assurance.

23. A method as in claim 22 wherein the electronic signals representing the transactional assurance are received in response to the sending of the request message.

24. A method as in claim 21 wherein the subscriber assurance comprises at least one of (a) an identification assurance of the identity of the subscriber and (b) an authorization assurance of authorization of the subscriber.

5 25. A method as in claim 21 wherein the reliance request message comes from the relying party.

10 26. A method as in claim 21 wherein the reliance request message comes directly from the relying party.

15 27. A method as in claim 21 wherein the electronic signals representing the transactional assurance are issued directly to the relying party.

28. A method as in claim 21 wherein the reliance request message includes certificate information derived from the transaction.

20 29. A method as in claim 27 wherein the determining whether to provide the transactional assurance further comprises:
determining the status of certificates associated with the transaction.